MN

Notice of Allowability	Application No.	Applicant(s)	
	10/763,867	CONOVER ET AL.	
	Examiner	Art Unit	
	Ronald Baum	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *5/21/2007*.

2. ☒ The allowed claim(s) is/are *1,3,4,6-24 and 26*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

8/1/07

DETAILED ACTION

Examiner's Statement of Reasons for Allowance

1. Claims 1, 3, 4, 6-24 and 26 are allowed over prior art.

2. This action is in reply to applicant's correspondence of 21 May 2007.

3. The following is an examiner's statement of reasons for the indication of allowable claimed subject matter.

4. As per claims 1, 21 and 26 generally, prior art of record, Baratloo, A., et al, 'Transparent Run-Time Defense Against Stack Smashing Attacks', 2000 Proceedings of the USENIX Annual Technical Conference, entire document, http://citeseer.ist.psu.edu/cache/papers/cs/24655/http:zSzzSzwww.research.avayalabs.comzSzprojectzSzlibsafezSzdoczSzusenix00.pdf/baratloo00transparent.pdf ('Baratloo'), fails to teach alone, or in combination, at the time of the invention, the features as discussed and remarked upon in the response of 21 May 2007 to office action of 12 March 2007.

Specifically, (as per claim 1, for example) prior art dealing with the ability to trace code for debugging, vulnerability hunting and malware analysis, insofar as trace buffer 'single stepping' through all instructions generally, and setting up for branch tracing more particularly (i.e., using Intel MSR registers to setup for tracing blocks of code delineated by branch instructions; pedram,'Branch Tracing with Intel MSR Registers', www.openrce.org/blog, 12/13/2006, entire blog, https://www.openrce.org/blog/view/535/Branch_Tracing_with_Intel_MSR_Registers), is generally known per se. Nowhere in the prior art is found collectively the *italicized* claim elements (i.e., the various aspects of stalling a critical OS function call prior to determination of a return instruction relative

to the function call within the last user to kernel branch trace record, and subsequent computer protective actions taken upon such determination), at the ***time** of the invention*, serving to patently distinguish the invention from said prior art;

"A method comprising:

stalling a call to

*a **critical*** operating system ***(OS) function***;

***determining** whether **branch trace records** of said **call** include*

*a **return** instruction* comprising:

locating

a most ***recent branch trace record** of*

said branch trace records;

searching

said branch trace records from

said most recent branch trace record

to locate

a user to kernel branch trace record of

said branch trace records; and

searching

*previous branch trace record **previous to***

said user to kernel branch** trace **record

for

said return instruction; and

taking protective action

to protect a computer system

upon a determination that

said branch trace records include

said return instruction.".

5. Dependent claims 3, 4, 6-20 and 22-24 are allowable by virtue of their dependencies.

Conclusion

6. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861 and unofficial email is Ronald.baum@uspto.gov. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at (571) 272-4195. The Fax number for the organization where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

8/1/07